GR 99 P 1259

3/pats

Description

User identification method

The invention relates to a method and a device for user identification for the unambiguous identification of a user or subscriber to a system.

Such a system can be, for example, a terminal such as a mobile telephone, or a building to which only certain persons should have access. However, it can also be a computer network which only allows access to certain data after unambiguous identification of the user, for example in on-line banking.

It is known that the user identifies himself by a personal identification number (PIN) only known to him in the ideal case. However, this method has the disadvantage that the user can easily forget or mistake the number due to the multiplicity of numbers to be used. The PIN number is, therefore, frequently noted in notebooks or the like which, however, entails a security risk.

For this reason, biometric identification methods have been recently developed in which biometric features of a user are used for the authentication. Such a biometric identification is a method for ensuring the allocation and the access of a certain person to a system or a location, which is not simple but is convenient and often very secure. Compared with the PIN code, the biometric identification has the advantage that it cannot be forgotten and the biometric features can be copied only by very elaborate means or not at all. This is because, whereas the PIN code is

pure software, there is always a more or less unambiguous correlation with the hardware, i.e. with the body of the respective user, in the case of biometric features. A possibility of such a

biometric identification consists in the acquisition of the fingerprint of a finger of the user. The latter places, for example, the right-hand thumb onto a contact area of an input device where the fingerprint patterns are detected with a resolution of approximately 50 µm. A computer unit compares the acquired fingerprint features such as branches or minuscules with the features of stored fingerprints of persons authorized for access. If there is a certain degree of correspondence which allows unambiguous identification of the user with very high probability, then use is allowed.

The problem with such fingerprint recognition systems is, however, that the finger, especially if it is contaminated, leaves on the sensor traces in the form of the fingerprint which, under certain conditions, can lead to recognition of the same authorized person during a new access authorization check without the finger having been applied again. For example, it is conceivable that using a glove or the like, pressure is exerted on the fingerprint sensor with the traces of the finger of the preceding authorized user and thus the authorized user is recognized again. This can result in possible misuse of the user identification.

The invention is, therefore, based on the object of proposing a method for user identification by means of biometric data, particularly fingerprint data, in which an erroneous identification due to remaining traces of a preceding identification process is prevented.

The object is achieved by an identification method having the following steps

(I) Acquisition of a biometric record of the user and the respective spatial position of the biometric data relative to a reference position,

(II) Storage of the biometric record and the associated position data,

(III) Reading out the biometric record and the associated position data of an identification process preceding the current identification process,

(IV) Comparison of the biometric data currently acquired and associated position data with the preceding biometric data and associated position data read out and rejection of the identification if the biometric data have a defined degree of correspondence and the position of the corresponding biometric data corresponds within a defined tolerance range.

The invention is based on the fact that, as a rule, a user is not able to position his finger during a new placement on the sensor with an accuracy of less than 100 µm in the vertical and horizontal direction. If a corresponding fingerprint with corresponding position is acquired during two successive identification processes, it is assumed that in the second identification process, the print traces remaining from the preceding identification process are being misused and access authorization is refused.

The invention also proposes a device for biometric user identification having the features of claim 8. Advantageous further developments of the method according to the invention and of the device according to the invention are described in the subclaims.

In an advantageous further development of the method, a mean value of the positions of a number of individual features of the biometric data is determined during the acquisition of the biometric record and, during the position comparison check of two successive identification processes, these mean position values

are compared with one another. Since the mean values are subject to less spread, for example due to a stretching or

compression of the surface of the skin or because of the acquisition raster of the pickup device, the tolerance range in which a position correspondence is evaluated as misuse, can be selected to be narrower in this variant of the method so that unwanted nonrecognition of a finger placed down correctly twice in succession becomes more improbable.

In the text which follows, the invention will be explained in detail by means of exemplary embodiments and referring to the drawings, in which

Figure 1 shows a diagrammatic block diagram of an exemplary embodiment of the device according to the invention,

Figure 2 shows a flowchart explaining an exemplary embodiment of the method according to the invention, and

Figure 3 shows a flowchart explaining a further exemplary embodiment of the method according to the invention.

Firstly, an exemplary embodiment of the invention will be explained with reference to the block diagram in Figure 1.

A fingerprint sensor 1 has a contact area 5 for placing a finger (indicated in dashed lines) and acquires the features such as branches or minuscules of the fingerprint. A position acquisition device 2 acquires the positions of these features relative to a reference position, for example a coordinate origin of an xy coordinate system of the contact area 5. The fingerprint data and associated position information thus determined are supplied to a memory 3 and a comparison device 4. From the memory 3, the corresponding fingerprint data and position data of the

preceding fingerprint acquisition are read out and also supplied to the comparison device 4. The fingerprint features and their positions are compared there, and in the case of a correspondence which is within a tolerance range, the comparison device 4 evaluates the current fingerprint acquisition or, respectively, the current

identification process as misuse of fingerprint traces of the last identification process and rejects access which is indicated on a display device 6.

In this method, the invention is based on the fact that

(1) old fingerprint traces are no longer of consequence when a new arbitrary finger is placed on the area, and are replaced by the new print, and

(2) a user will not be able to position his finger, when placing it down again, with such accuracy that the finger corresponds to the preceding fingerprint within up to 100 µm or 50 µm in position and direction.

Since the position of the remaining traces of the earlier fingerprint of the preceding identification process cannot shift in space with respect to the sensor, it is not only the individual features of the fingerprint such as branches or minuscules but also their precise position on the contact area which are stored in the present invention, for example as xy coordinates or as polar coordinates. If, in the case of a new fingerprint of a new identification process, corresponding features lie within a tolerance range of 50 µm or 100 µm at the same spatial position, it is highly probable that this is not a new placement of a finger of the same person but the features of the last print. In this case, access authorization or identification must be refused and the user must be requested to place his finger again.

An exemplary embodiment of the method according to the invention will now be explained with reference to the flowchart of figure 2.

In a step S1, the biometric data and their associated positions on the contact area are acquired. In a step S2 these are stored for use

in the user identification process following next. In step 3, accordingly, the biometric data and associated positions of the preceding identification process are read out. In step S4, a comparison is made to determine whether the features and positions of the two successive acquisitions, i.e. the fingerprint acquisition of the current user identification process and the fingerprint acquisition of the immediately preceding user identification process correspond with each other. If both the features of the fingerprint have a defined degree of correspondence and the positions of these features correspond to one another within a tolerance range of 50 µm or 100 µm, the identification is refused (step S5), otherwise, the check continues to step S6 in which a check is made, as in known user identification methods, to determine whether the features of the current acquisition of the fingerprint correspond to the stored features of fingerprints of certain persons, for example authorized users. If this is not so, identification is refused (step S7), otherwise, identification takes place.

The variant of the method explained in figure 3 differs from that shown in figure 2 in that a mean value of the positions of acquired features of the biometric record (fingerprint) is calculated and stored in a step S11. In step S4, it is then not the positions of individual features of the fingerprints but the mean position values of the current fingerprint acquisition and the preceding one which are compared with one another. This has the advantage that statistic deviations due to stretching or compression of the skin or due to the pixel spacing of the contact area 5 of the fingerprint sensor are averaged out so that the tolerance range can be selected to be smaller, for example 10 µm to 20 µm. This reduces the probability of unjustified rejections of the identification.

The invention provides an improved method for biometric user identification in which misuse due to fingerprint traces of a preceding user identification which are remaining on the acquisition device can be prevented. The invention can be applied to checking the authorization to use devices such as, for example, mobile telephones or for identifying a computer user in bank transactions. However, other applications are also conceivable in which the identity of a person must be reliably established on the basis of biometric data such as, for example, a fingerprint.